Correio Electrónico
Microsoft Exchange

Manual de Utilização e Configuração

Sumário

Caixas de Correio Individuais

Configurações de acesso

Configurações de acesso **Microsoft Exchange**	**Webside** **PT Prime**	**Telepac (*)** **SAPO (*)**
WEBMAIL	http://webmail.webside.pt https://webmail.webside.pt http://mail.ptprime.pt https://mail.ptprime.pt	http://exchange.telepac.pt https://exchange.telepac.pt http://exchange.sapo.pt
POP	pop.webside.pt pop.mail.ptprime.pt	pop.exchange.telepac.pt pop.exchange.sapo.pt
SMTP (**)	smtp.webside.pt smtp.mail.ptprime.pt	smtp.exchange.telepac.pt smtp.exchange.sapo.pt
IMAP	imap.webside.pt imap.mail.ptprime.pt	imap.exchange.telepac.pt imap.exchange.sapo.pt
Configurações de acesso “Microsoft Exchange ActiveSync“	**Servidor:** webmail.webside.pt mail.ptprime.pt **Domínio:** asp-telepac	**Servidor:** exchange.telepac.pt exchange.sapo.pt **Domínio:** asp-telepac

- (*) Estas instruções são apenas aplicáveis a clientes Telepac e SAPO com caixas de correio Microsoft Exchange personalizadas com o domínio do cliente.
- (**) SMTP autenticado
    - Necessária configuração de Username e Password

Consola de configuração Online

Através desta ferramenta poderá personalizar a sua caixa de correio:

- Contactos do Cliente
- Cartão de Visita
- Personalização do “Display Name” (Nome associado ao endereço)
- Configurações de acesso

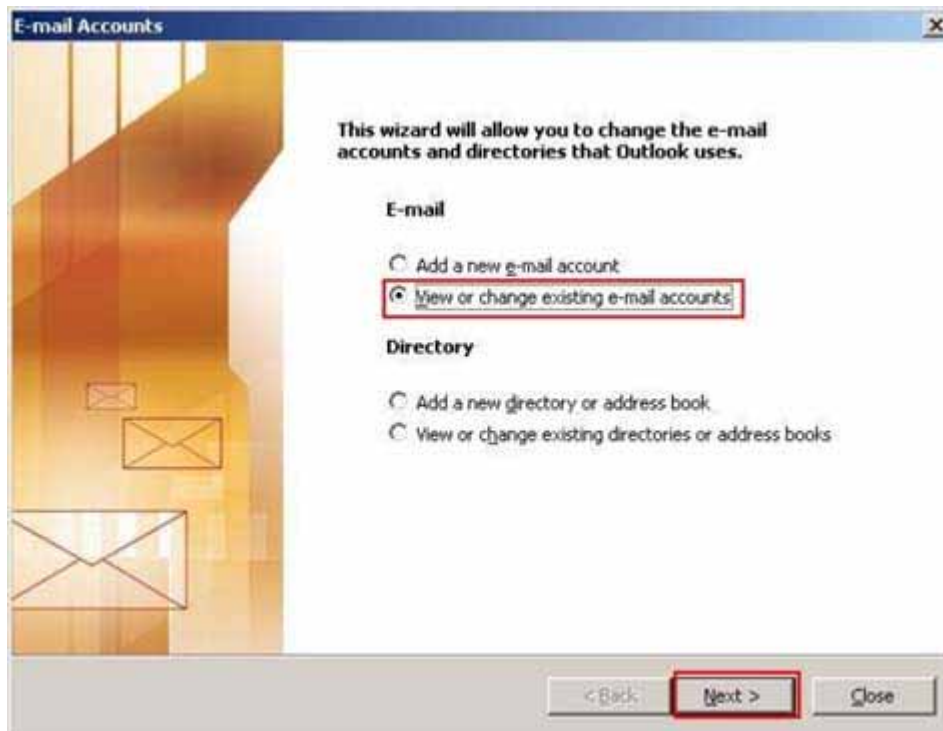
Configure a sua caixa de correio individual através do seguinte endereço:

- Clientes PTPrime: http://consola.mail.ptprime.pt
- Clientes Telepac: http://consola.exchange.telepac.pt
- Clientes SAPO: http://consola.exchange.sapo.pt
    - Para aceder, introduza o endereço da sua Caixa de Correio Individual e a sua Password

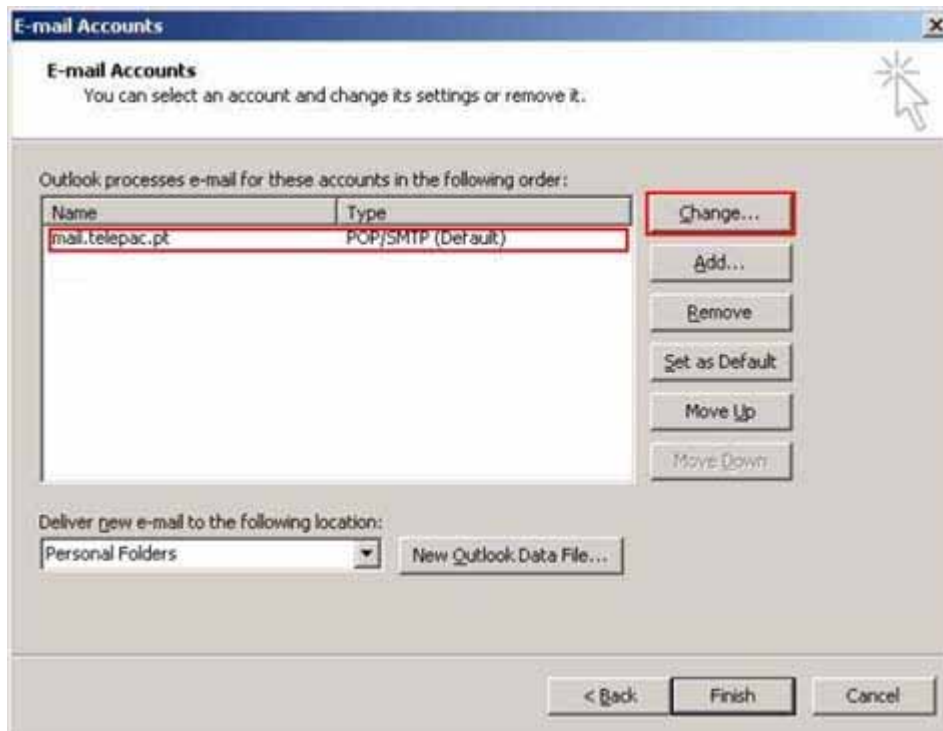
Se utiliza o programa de mail Microsoft Outlook, necessita de efectuar as seguintes configurações de acesso à sua caixa de correio individual:

Passo 1

O primeiro passo é abrir a opção "Email accounts".

No Desktop, clique com o botão direito do rato sobre o icon do Microsoft Outlook, ou alternativamente, directamente no Microsoft Outlook, na opção " Tools" e de seguida escolha a opção "E-Mail Accounts..."

Nesta janela escolha a opção " View or change existing e-mail accounts" e clique em " Next".

Passo 2

Irá aparecer a janela onde tem configurado as suas contas de Mail:

Nesta janela seleccione a conta que corresponde à sua caixa de correio e clique em " Change...".

Nota: Caso esteja a instalar pela primeira vez clique em "Add..." para criar uma nova configuração de acesso à sua caixa de correio.

Passo 3

Irá aparecer a janela de configurações a sua caixa de correio:

ATENÇÃO:

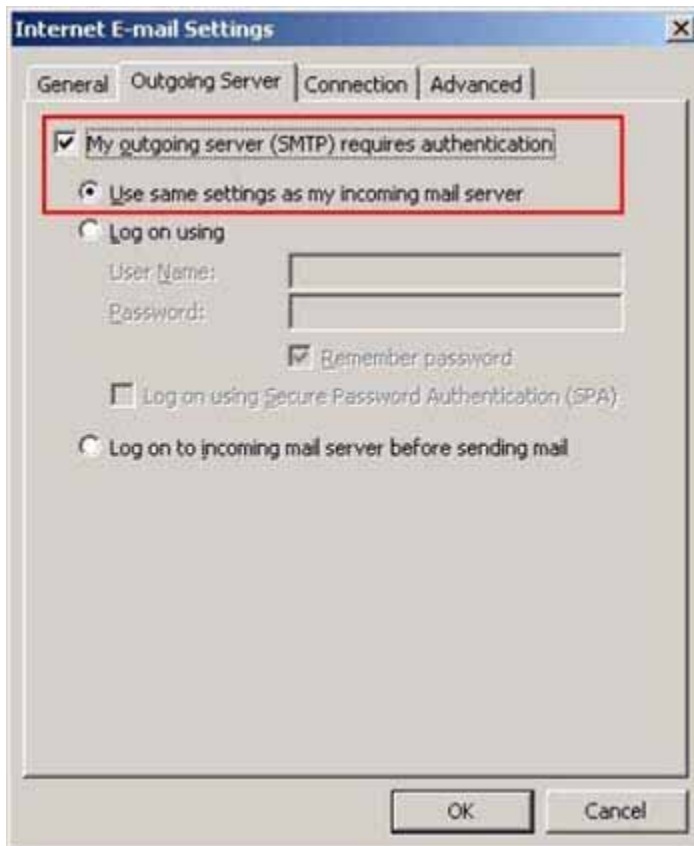
Deverá introduzir as configurações correctas de acesso à sua Caixa de Correio nas caixas assinaladas a vermelho, nomeadamente:

- Servidor POP3 (Para recepção do E-Mail)
- Servidor SMTP (Para envio do E-Mail)
- Username (Deverá adicionar o domínio ao qual a sua caixa de correio está associada)
- Password (Nunca divulgue a sua password)

Verifique quais as configurações correctas !

Após ter efectuado estas alterações terá que clicar em: " More Settings..." e siga as instruções.

Passo 4

Irá aparecer a janela de configurações de autenticação:

Terá de obrigatoriamente seleccionar a opção "My outgoing server (SMTP) requires authentication" e de seguida " Use same settings as my incomming mail server".

Após ter efectuado as alterações necessárias clique em "OK".

Para que todas as novas configurações fiquem guardadas após ter clicado em "OK", clique em "Next >" para finalizar as alterações.

Caixas de Correio Corporativas

Pré Requisitos

ATENÇÃO:

- (*) Para que possa usar o protocolo MAPI é necessário certificar-se que o seu computador corresponde aos seguintes pré-requisitos:
  - Microsoft Windows XP SP1 com o **Update 323166** ou SP2 sem Update
  - Microsoft Outlook 2003
- (**) Autenticação:
  - Necessária configuração de Username e Password
  - Username = Alias Principal. Exemplo: meu-nome@meu-dominio.pt

Update 323166: http://support.microsoft.com/?kbid=331320

Configurações de acesso

Configurações de acesso **Microsoft Exchange**	**PTPrime**
WEBMAIL (**)	http://mailempresa.ptprime.pt
EXCHANGE MAPI (*)	mailempresa.ptprime.pt
POP	pop.mailempresa.ptprime.pt
SMTP (**)	smtp.mailempresa.ptprime.pt
IMAP	imap.mailempresa.ptprime.pt
Configurações de acesso “Microsoft Exchange ActiveSync“	**Servidor:** mailempresa.ptprime.pt **Domínio:** asp-telepac

Consola de configuração Online

Através desta ferramenta poderá personalizar a sua caixa de correio:

- Contactos do Cliente
- Cartão de Visita
- Personalização do “Display Name” (Nome associado ao endereço)
- Configurações de acesso

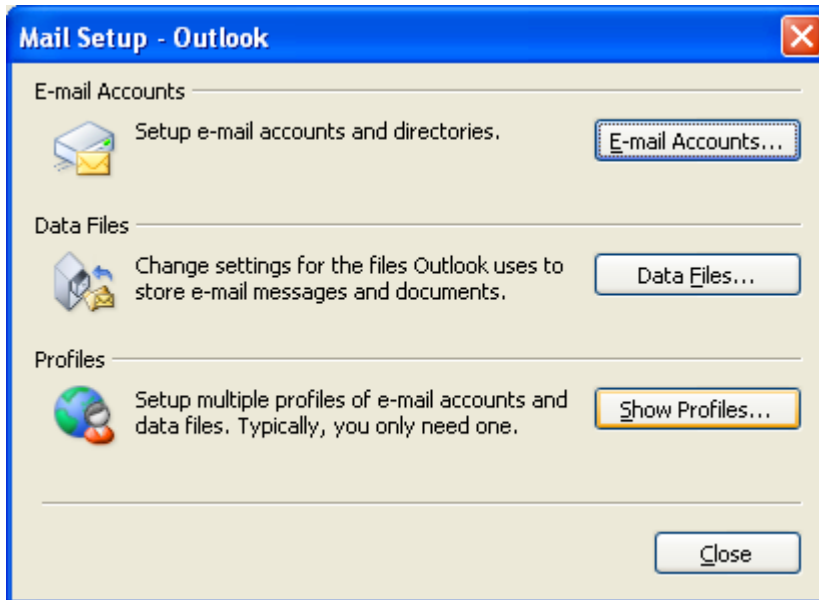
A conta de Correio Corporativa configurada como “Administrador” poderá proceder a definições adicionais nas restantes contas de Correio Corporativas.

Aceda através do seguinte endereço:

- PTPrime: http://consola.mailempresa.ptprime.pt
  - Para aceder, introduza o endereço da sua Caixa de Correio Corporativa e a sua Password

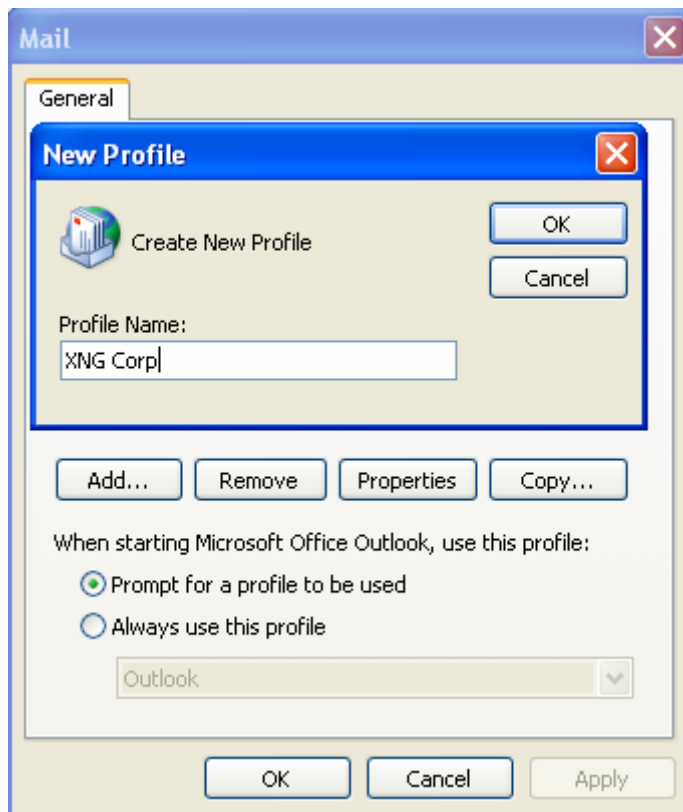
Se utiliza o programa de mail Microsoft Outlook 2003, necessita de efectuar as seguintes configurações de acesso à sua caixa de correio corporativa:

Passo 1

Através do "Painel de Controlo" seleccione a opção "Mail".
Será apresentado o seguinte ecran:

Certifique-se que cria um novo "Perfil" para esta nova Caixa de Correio Corporativa (Microsoft Exchange Server).

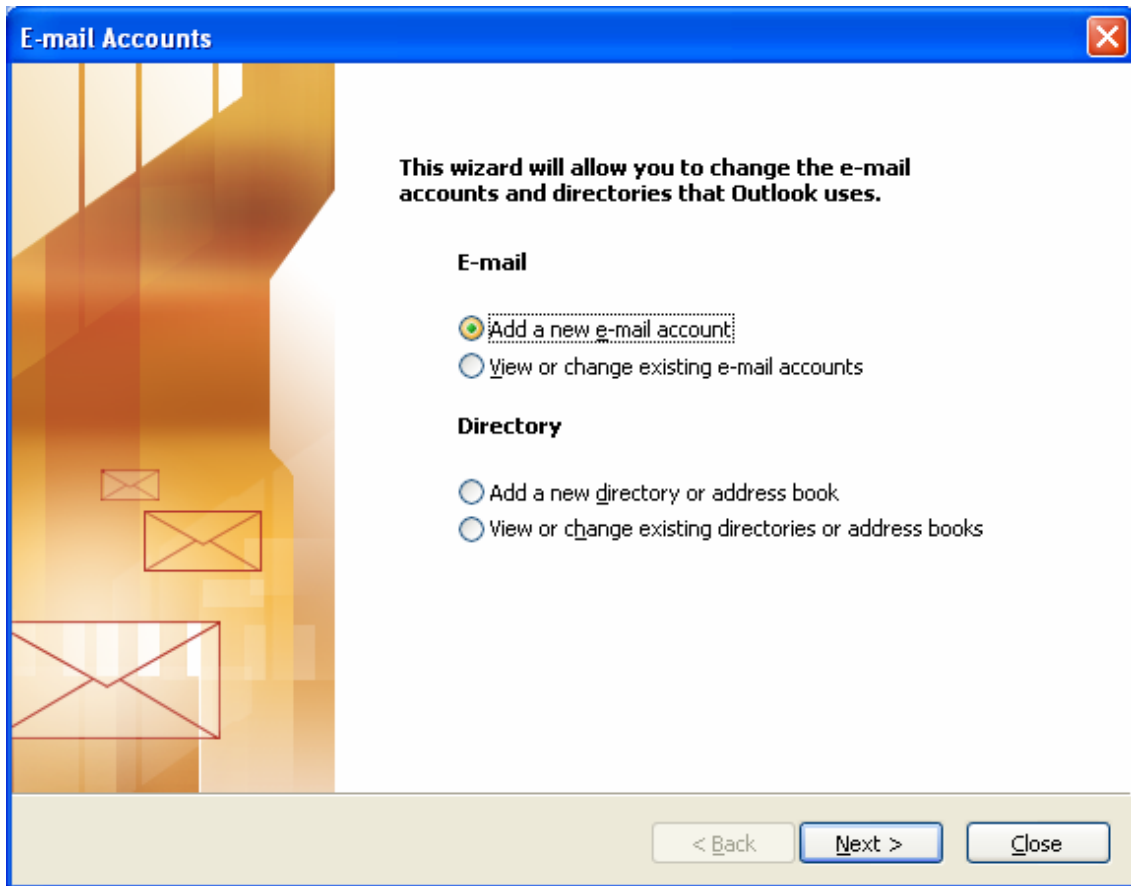
Passo 2

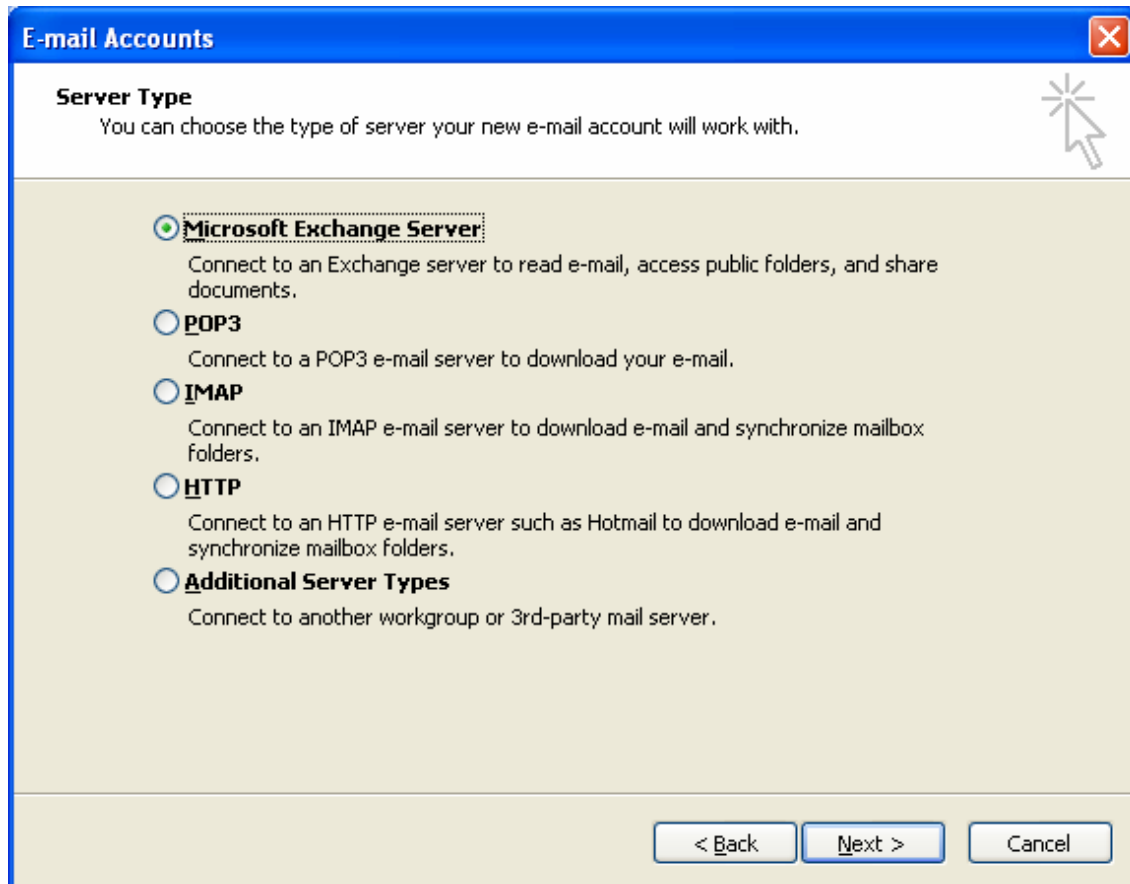
Uma vez que vai criar uma ligação a um servidor Exchange, será necessário criar um novo “Perfil”. Isto deve-se ao facto de, eventualmente, no perfil já existente, existirem caixas de correio já configuradas.
Um “Perfil” com uma ligação a um servidor Exchange apenas permite uma única caixa de correio.

Seleccione o nome para o seu novo “Perfil”:

Recomendamos que o novo “Perfil” proceda à entrega do correio num novo ficheiro .PST, diferente do que eventualmente já exista.

Passo 3

Crie a ligação ao servidor Exchange no novo "Perfil" criado.

Seleccione a opção "Add a new e-mail account":

Passo 4

Seleccione o tipo de caixa de correio a criar no seu novo “Perfil”.
A opção a seleccionar é “Microsoft Exchange Server”:

Passo 5

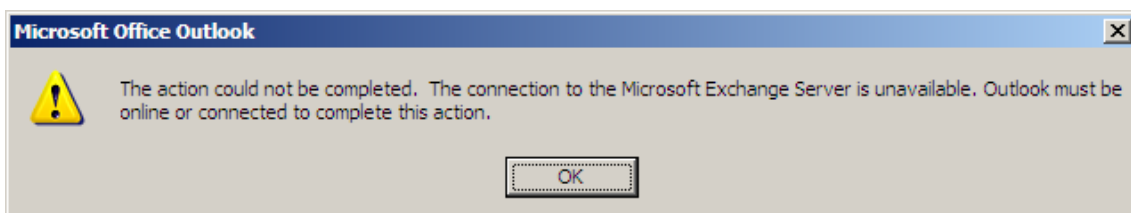
Preoceda à configuração de acesso ao servidor Microsoft Exchange.

Introduza o seu username e seleccione a opção “More Settings...”:

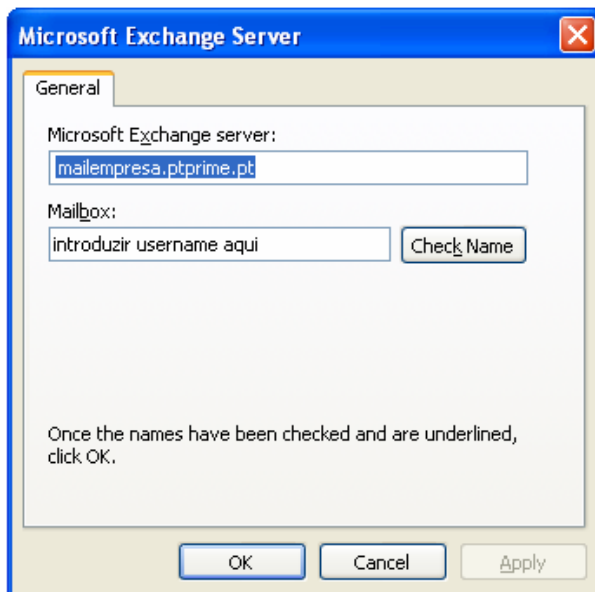
Introduza as seguintes configurações:

- Microsoft Exchange Server: **asp-exc04.asp-telepac.local**
- User Name: alias@dominio.pt (EXEMPLO)

Seleccione a opção **“More Settings…”**;

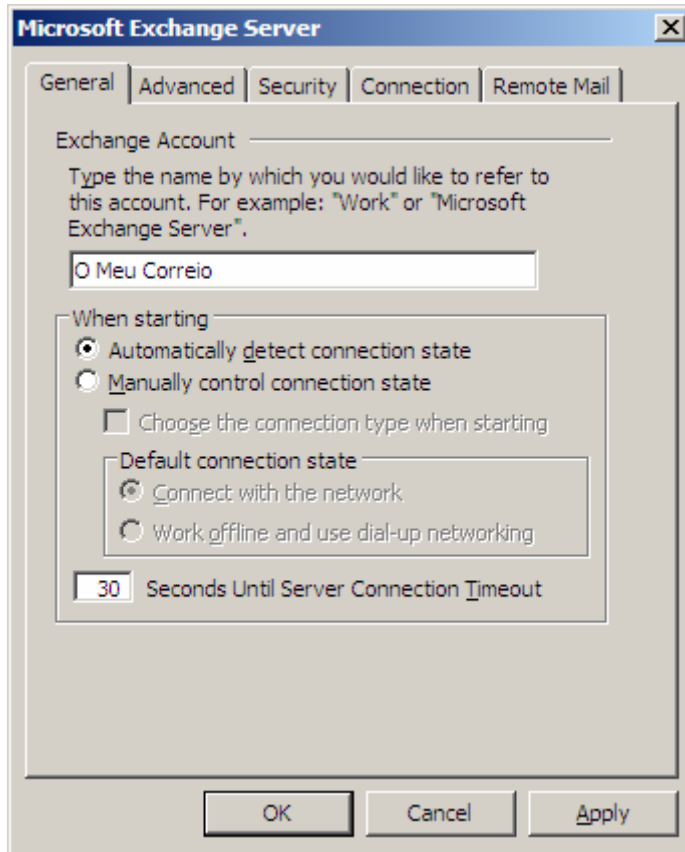
Deverá aparecer a seguinte mensagem:

Seleccione a opção “OK”

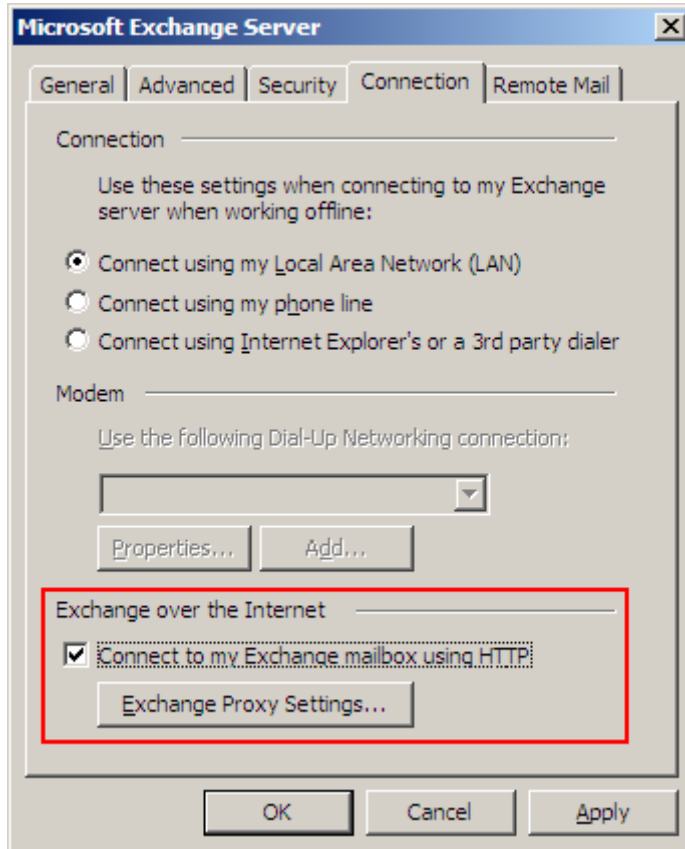
Passo 6

Quando solicitado, introduza a o user e a password.

Introduza: mailempresa.ptprime.pt (ou o seu nome)

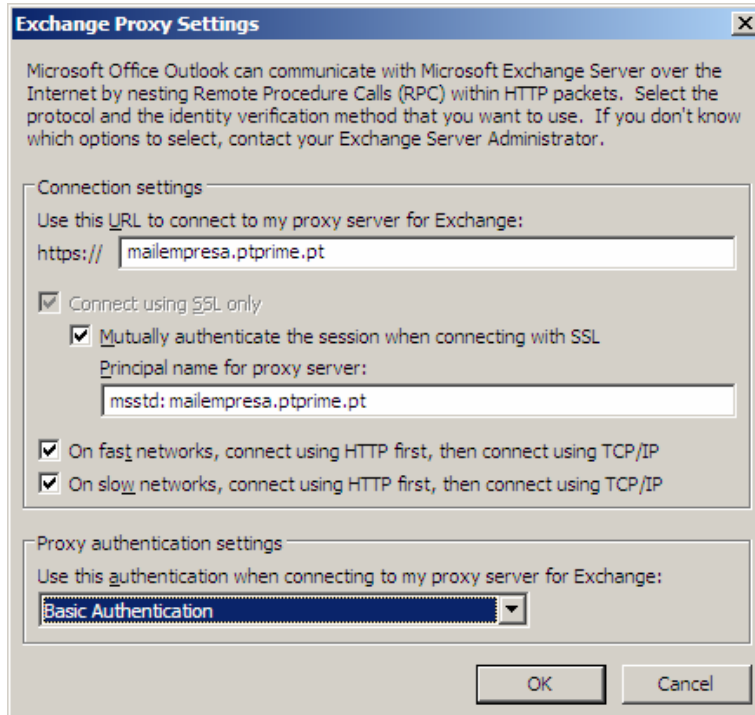
Neste ecran deverá seleccionar a opção "**Cancel**" para aceder as configurações avançadas

Passo 7

Neste ecran seleccione a pasta **“Connection”**.

Passo 8

Deverá preencher a pasta "Connection" como exemplificado na imagem e de seguida seleccionar a opção **"Exchange Proxy Settings…"**

Passo 9

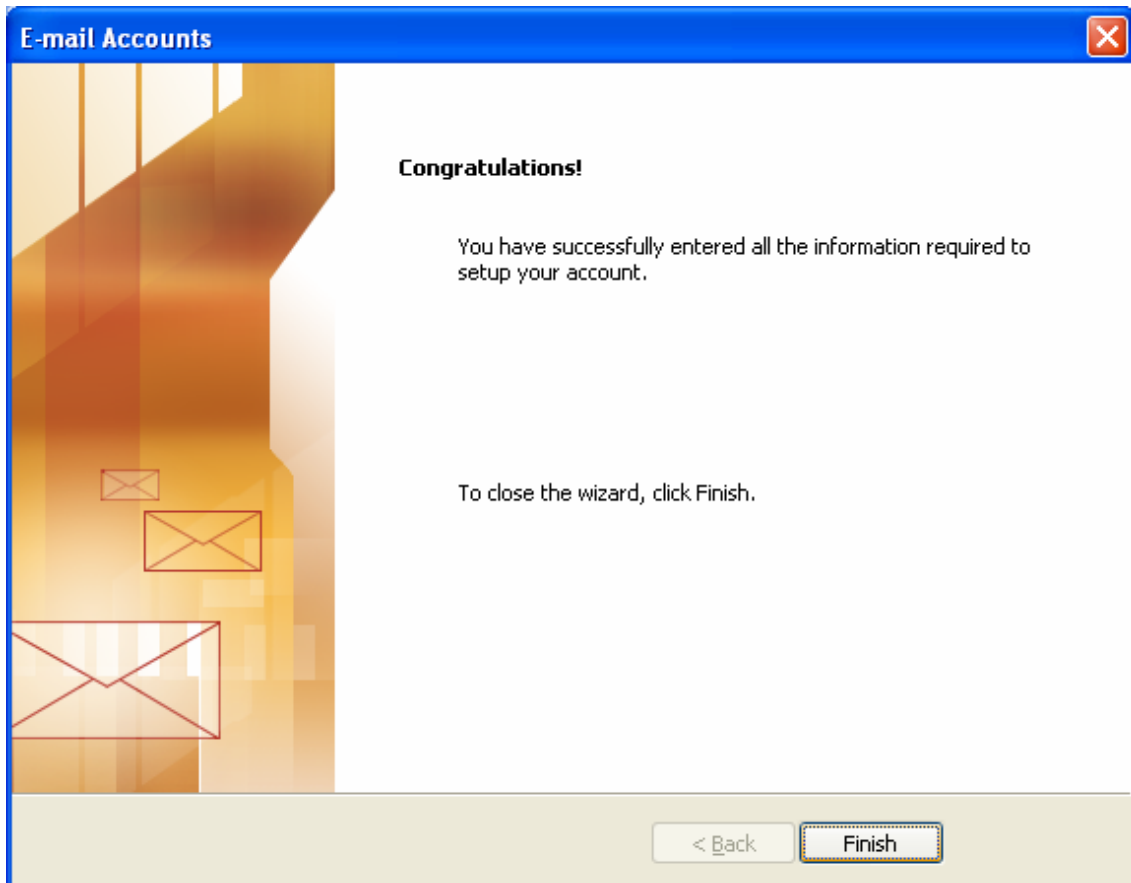
Introduza os dados referentes ao Exchange Proxy Server, de acordo com a imagem em baixo apresentada e seleccione a opção “OK”

Introduza:

https://mailempresa.ptprime.pt

msstd:mailempresa.ptprime.pt

Passo 10

Parabéns.
Acabou de efectuar uma ligação com sucesso à sua Caixa de Correio Corporativa.

Seleccione a opção “Finish” e abra o Microsoft Outlook 2003 com o “Perfil” previamente criado.

Microsoft Exchange ActiveSync

A plataforma de Correio Electrónico Empresarial do Grupo PT é suportada em servidores Microsoft Exchange Server.

Pode sincronizar as mensagens de correio electrónico, os itens de calendários, contactos, notas e tarefas do Outlook com o Pocket PC utilizando o Microsoft ActiveSync®.

O ActiveSync permite criar uma parceria entre o Pocket PC e o computador de secretária utilizando um cabo, um dispositivo de ancoragem ou infravermelhos.
Depois de estabelecer a parceria, pode sincronizar os dados utilizando um modem ou uma placa de rede (Ethernet) caso o Pocket PC suporte este dispositivo.

Pode também utilizar o computador para estabelecer ligação com outros recursos através do ActiveSync. Pode sincronizar informações entre o dispositivo móvel e um servidor caso a empresa tenha instalado o Microsoft Exchange Server com o Exchange ActiveSync.

Para sincronização via PC, necessita de:

1. ActiveSync 3.7.1 instalado (ou versão superior);
2. Um suporte de ancoragem, cabo para sincronização disponível, Bluetooth, ou Infra-Vermelhos.
3. Acesso à Internet

Para sincronização via GPRS, necessita de:

1. Terminal móvel com GPRS activo e configurado

Nota: Caso necessite de apoio adicional, por favor consulte:
http://www.tmn.pt/servicos/acesso_internet/acesso_email/descricao.shtml

De seguida apresentamos as configurações necessárias para que proceda à sincronização da sua caixa de correio Telepac ou PTPrime.

Configurações de acesso

Caso pretenda configurar a utilização do ActiveSync num terminal móvel, siga as seguintes instruções:

Passo 1

Seleccione a aplicação “ActiveSync”

Passo 2

Ao executar o ActiveSync, ser-lhe-á apresentado o seguinte ecrã.

Existem várias formas de se conectar. Antes de proceder à sincronização, certifique-se que está a utilizar uma das formas possíveis para estabelecer a parceria. Exemplos: Cabo USB, ligação via GPRS, etc. e que o equipamento possua acesso à Internet.

Passo 3

Seleccione no menu “Tools” a opção “Options”:

Passo 4

Clientes PTPrime ou Telepac (com caixas de correio de domínio próprio)

Configuração do servidor: **webmail.webside.pt** (ou mailempresa.ptprime.pt)

Nota: este serviço não se encontra disponível a clientes Telepac com contas de correio "@mail.telepac.pt"

Passo 5

Introduza o username e password de acesso à sua caixa de correio.

Utilize como Domínio: **asp-telepac**

Seleccione “OK”

Nota:
Os clientes Telepac devem introduzir o username da seguinte forma:
Exemplo: op123456@dominio.pt **(Utilizar apenas como username: op123456)**

Passo 6

Seleccione a opção "Sync" de forma a dar inicio à sincronização da sua caixa de correio Microsoft Exchange.

Passo 7

Parabéns, a partir deste momento o seu terminal móvel encontra-se sincronizado com a sua caixa de correio Exchange

ANTI-SPAM

Gestor de Mensagens Electrónicas de Publicidade Abusiva da Microsoft: **IMF**

O que significa SPAM ?

SPAM é o envio de Mensagens Electrónicas não solicitadas pela Internet.
Do ponto de vista de quem envia SPAM, é uma forma de envio massivo de mensagens, para uma lista de milhares de endereços de E-mail. Do ponto de vista de quem recebe SPAM, normalmente esse tipo de mensagens é considerado "Lixo Electrónico".
Os Spammers tipicamente enviam mensagens para milhões de endereços de E-mail devido aos baixos custos associados, na expectativa de que uma pequena parte dos receptores respondam à sua oferta.
O SPAM tornou-se no maior problema dos utilizadores da Internet.
'Commercial Electronic Mail Messages' são mensagens informativas de uma determinada entidade, que pretende divulgar um determinado produto, divulgar uma promoção, ou enviar a sua newsletter a todos os clientes que subscreveram este tipo de serviço.
O grande problema que reside com este tipo de mensagens, é que a grande maioria de este tipo de mensagens, que circula na Internet, não foi subscrito pelo destinatário, o que passa a ser classificado como E-mail não solicitado, vulgarmente conhecido como SPAM.

Bloqueio de Mensagens Electrónicas de Publicidade Abusiva e Filtragem de Conteúdos com Base no Servidor para Empresas

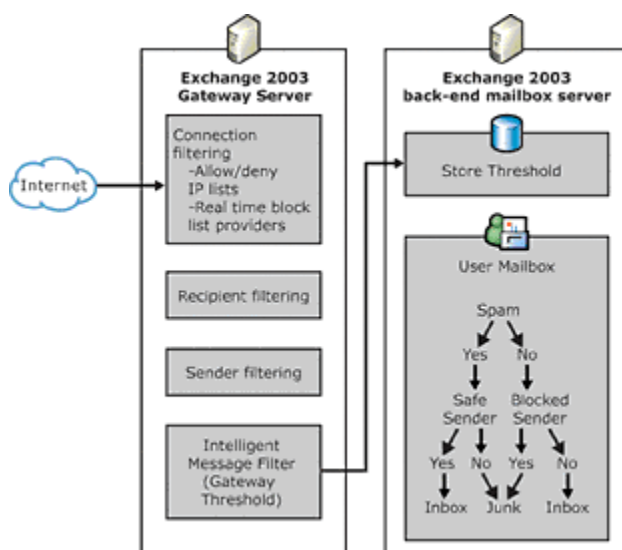
O Gestor de Mensagens Electrónicas de Publicidade Abusiva é uma componente de bloqueio de mensagens electrónicas de publicidade abusiva e de filtragem de conteúdos de elevado desempenho e de nível empresarial especificamente concebido para ajudar os administradores a reduzir o impacto destas mensagens e do tráfego de mensagens de correio não solicitado nas suas redes.

A Necessidade Crescente de Prevenção das Mensagens Electrónicas de Publicidade Abusiva

As mensagens electrónicas de publicidade abusiva estão a aumentar e tornaram-se rapidamente um transtorno para os utilizadores empresariais e os recursos das redes, comprometendo também os recursos financeiros. Idênticos em vários aspectos à ameaça dos vírus, as organizações demonstram-se hesitantes em relação ao acréscimo de sistemas, serviços e produtos de filtragem concebidos para reduzir este fluxo de tráfego não solicitado. As empresas necessitam de soluções que reduzam de forma significativa a massa de mensagens electrónicas de publicidade abusiva e de correio não solicitado, limitando simultaneamente os alarmes falsos que podem contribuir para a perda de comunicações valiosas.

O Custo Crescente das Mensagens Electrónicas de Publicidade Abusiva

De acordo com um estudo recente do Ferris Group, realizado em Janeiro de 2003: "Controlo das Mensagens Electrónicas de Publicidade Abusiva: Problemas e Oportunidades", as mensagens electrónicas de publicidade abusiva representam quase 40% de todas as mensagens de correio electrónico que entram na empresa média. Calcula-se que, em 2003, as empresas terão de pagar até 10 mil milhões de dólares em encargos derivados de mensagens electrónicas de publicidade abusiva.

Esquema de funcionamento:

As principais features do Intelligent Message Filter são as seguintes:

- Análise de mensagens baseada em Heurísticas para determinar se um mail deve ser classificado com SPAM ou legítimo;
- Capacidade de adaptação ao longo do tempo de modo a apanhar mensagens não desejadas e prevenir falsos positivos;
- Integrado na ferramenta de Administração do Exchange 2003;
- Suporte a classificações de Spam Confidence Level (SCL) por mensagem;
- Utiliza tecnologia da Microsoft Reasearch para classificar a probabilidade de cada mensagem ser UCE através do SCL;
- O SCL é um valor normalizado assignado a uma mensagem que indica, baseado nas características da mensagem (conteúdo, header,…), a probabilidade de uma mensagem ser SPAM.

Existem onze valores disponíveis para categorizar SPAM:

SCL	Categorização de SPAM
-1	Reservado a mensagem submetidas internamente. Um valor de -1 é sempre atribuído a mensagens submetidas internamente e nunca deve ser modificado.
0	Mensagens que não são SPAM.
1	Probabilidade muito baixa da mensagem ser SPAM
2-8	Níveis intermédios
9	Probabilidade muito alta da mensagem ser SPAM

Mais informações sobre o SCL e IMF (em Inglês) podem ser obtidas em:
http://www.microsoft.com/exchange/downloads/2003/imf/default.mspx

ANTI-VIRUS

Antivírus e Filtragem de Conteúdos para Exchange

O Antigen para Microsoft Exchange da Sybari oferece uma linha de defesa prévia contra a propagação de vírus, worms e código malicioso por correio electrónico. O Antigen é uma solução antivírus ao nível do servidor que proporciona uma protecção exaustiva através da nossa abordagem de múltiplos motores de análise, bem como capacidades avançadas de filtragem de conteúdos.

Tecnologia Avançada, Protecção Inovadora
O Microsoft Exchange oferece aos utilizadores do Outlook o poder da colaboração. Esta robusta solução integral para serviços de mensagens e de colaboração permite aos utilizadores do Outlook comunicar e partilhar dados e documentos através de correio electrónico. Contudo, ao mesmo tempo que partilham informações, os utilizadores do Outlook têm também a capacidade de receber e distribuir vírus, worms e código malicioso transportados por correio electrónico - danificando os valiosos dados da sua empresa e comprometendo a rede.

Os administradores do Microsoft Exchange têm uma solução: o Antigen da Sybari. O Antigen é uma solução abrangente de antivírus, filtragem de conteúdos e segurança de correio electrónico especificamente concebida para suprir as necessidades de segurança dos administradores do Microsoft Exchange. O Antigen detecta, bloqueia, filtra e elimina vírus antes de eles poderem chegar a aplicações demissão crítica, sem comprometer a integridade dos seus servidores de serviços de mensagens e de colaboração.

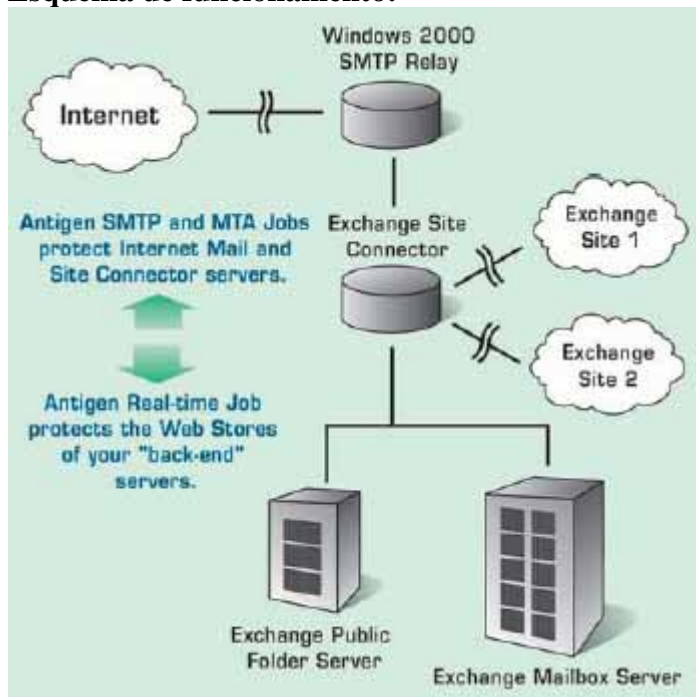
Um Leque de Características Poderosas

Protecção Prévia.

Enquanto que os produtos antivírus tradicionais analisam as mensagens de correio electrónico e respectivos anexos em relação a vírus nocivos depois de estes terem chegado a uma parte sensível da rede, o Antigen utiliza uma abordagem mais inovadora: o mesmo faz uma análise automática e desactiva ameaças contidas no cabeçalho, corpo e anexos das mensagens em múltiplos pontos de análise antes de estas chegarem às caixas de correio dos utilizadores e causarem danos irreparáveis.Com a sua abordagem pró activa à análise e filtragem de mensagens de correio electrónico e documentos, o Antigen adianta-se assim na detecção de possíveis ameaças, garantindo a máxima protecção para os seus servidores de serviços de mensagens e de colaboração. Uma

Velocidade Notável Conjugada com um Desempenho Incrível.

A tecnologia exclusiva de análise"na memória" do Antigen permite-lhe realizar uma análise mais rápida - minimizando assim o impacto operacional sobre o seu servidor Exchange. Além de analisar a zona de Armazenamento de Informação, o Antigen também analisa as mensagens de correio SMTP recebidas e enviadas pelo conector Internet Mail Service (IMS) do Microsoft Exchange no Exchange 5.5 ou no módulo de transporte SMTP para o Exchange 2000 no Windows 2000.A Tarefa de Análise de MTA do Antigen também analisa o tráfego de mensagens que atravessa o MTA do Exchange 2000,incluindo X.400 e outro tráfego de ligação. Ao distribuir a análise de vírus por vários servidores e por múltiplos pontos em cada servidor Exchange, o Antigen ultrapassa as expectativas dos administradores no tocante à protecção e eficiência dos servidores.

Esquema de funcionamento:

A arquitectura original do Antigen faz uma análise fiável, em tempo real, de 100% das mensagens e dos objectos que são escritos na zona de Armazenamento de Informação.

- Antigen oferece modos seleccionáveis, incluindo suporte completo da API de Análise de Vírus da Microsoft (VS API2.0/VS API 2.5) para Exchange 2000 e Exchange 2003.
- Antigen detecta possíveis ameaças à segurança antes de estas poderem chegar às caixas de correio electrónico dos utilizadores.
- Antigen recorre a motores de análise múltiplos de forma a proporcionar uma maior protecção com um impacto mínimo nos servidores das empresas.
- Antigen proporciona a filtragem de anexos e bloqueia mensagens por assunto, remetente ou nome de domínio. Uma vez detectados, os ficheiros podem ser colocados em quarentena, eliminados ou depurados.
- Antigen é uma solução única para Exchange 5.5,Exchange 2000 e Exchange 2003
- Antigen proporciona textos de desresponsabilização que indicam que o correio enviado foi sujeito a análise antivírus.

> "O Antigen detectou cinquenta e uma mil cópias do vírus "love" nas primeiras 24 horas em que o vírus atacou servidores de correio em todo o mundo. A minha equipa utilizou a funcionalidade de Filtragem de Ficheiros do Antigen, que funcionou de modo brilhante".
>
> Mark Moynes, Nortel Networks

Opções Sofisticadas de Análise.
O Antigen proporciona aos administradores uma variedade de ferramentas e de opções que resultam em elevado valor, flexibilidade e desempenho aperfeiçoado.

- Análise em tempo real, programada e "a pedido" de múltiplos Grupos de Armazenamento e respectivas bases de dados.
- Protecção total do Sistema de Armazenamento na Web do Exchange e do Outlook Web Access (OWA).
- Múltiplas tarefas de análise e múltiplos processos em tempo real asseguram uma protecção de redundância e um elevado desempenho.
- A análise de mensagens de MTA protege todas as mensagens encaminhadas através dos Conectores de MTA do Exchange (X.400,MS Mail,CC Mail,etc.)

Integração da API de Análise de Vírus para Exchange 2000 e Exchange 2003.
O Antigen proporciona suporte para a API de Análise de Vírus da Microsoft, oferecendo aos administradores uma solução global para ambientes mistos. Agora, é possível configurar análises em tempo real e manuais para utilizar as implementações ESE ou VS API 2.0 e 2.5 para o Exchange 2000 e Exchange 2003,ao mesmo tempo que utiliza o ESE para o Exchange 5.5 (sem restrições de "service pack").Uma solução única para todas as plataformas Exchange garante uma protecção óptima durante migrações de servidores a partir de versões prévias do Exchange.

Gestão de Múltiplos Motores de Análise.
O Antigen proporciona suporte para múltiplos motores de análise de vírus com cinco das principais tecnologias de motores de análise da Kaspersky Labs, Sophos, Norman Data Defense e dois motores antivírus eTrust da Computer Associates. O gestor de múltiplos motores de análise está disponível para todas as tarefas de análise do Antigen e permite aos administradores personalizar e configurar uma variedade de definições e opções a cada nível.

Concebido para Proporcionar o Máximo Desempenho.
De forma a evitar o consumo de recursos e a melhorar o desempenho da análise, as mensagens são analisadas "na memória" em vez de serem enviadas para o disco. Os múltiplos motores de análise utilizam a cache na memória para maximizar o desempenho durante a análise de ficheiros. Os administradores têm controlo total sobre as opções e podem configurar a utilização de motores de análise de forma adequada para o seu ambiente.

Administração Central.
O Antigen está preparado para ambientes empresariais e pode ser facilmente instalado e desenvolvido a partir de um único local para todos os servidores Exchange.
A configuração e controlo de todas as operações e bases de dados de quarentena do Antigen podem ser efectuados a partir de uma localização centralizada, utilizando o Antigen Central Manager (ACM),o Cliente Antigen e o controlo Active X do Antigen.

Filtragem de Ficheiros do Antigen (Antigen FileFiltering™ (AFF)).
A funcionalidade AFF filtra todas as mensagens com anexos recebidas e enviadas por extensão de ficheiro, tipo, nome ou caracteres universais e proporciona opções para colocar em quarentena, eliminar ou depurar ficheiros eliminados com problemas. Os anexos também podem ser bloqueados com base no tamanho do ficheiro.

Filtragem de Conteúdos do Antigen.
Bloqueie mensagens recebidas ou enviadas com base no assunto ou em caracteres universais, remetente ou nome de domínio. O Antigen coloca em quarentena e/ou elimina as mensagens, como for desejado.

Gestão de Mensagens Electrónicas de Publicidade Abusiva do Antigen.
Integra-se totalmente com o Gestor de Mensagens Electrónicas de Publicidade Abusiva da Sybari opcional para bloquear as mensagens electrónicas de publicidade abusiva por filtragem de assunto, remetente e domínio, integração de múltiplas "listas negras",integração de "listas brancas",pesquisa de DNS e filtragem por palavras-chaves baseada em regras no corpo da mensagem. Estas mensagens podem ser colocadas em quarentena, eliminadas, marcadas e/ou depuradas, como for desejado.

Depuração Automática de Worms.
O AntigenWorm Purge™ permite aos administradores eliminar completamente mensagens de correio electrónico que contenham worms conhecidos antes de as mesmas entrarem na zona de Armazenamento da Web do Exchange. Isto ajuda a reduzir os volumes de chamadas telefónicas para os centros de apoio técnico, bem como a propagação de mensagens electrónicas de publicidade abusiva gerada por worms.

Actualizações Automáticas.
As assinaturas de vírus são automaticamente actualizadas de forma a garantir que os vírus mais recentes são imediatamente detectados. Todos os servidores Exchange podem ser configurados para transferir e actualizar os seus motores de análise através de um único servidor designado.

Serviços de Aviso e de Quarentena.
Utilizam serviços de mensagens personalizados do Exchange para a emissão de avisos de incidentes relacionados com vírus e eventos do Antigen,tais como a conclusão de uma Tarefa de Análise Manual. A actividade dos vírus é controlada a partir de uma consola do Antigen, do ACM, de um registo do NT ou de um ficheiro de texto. O Antigen possui uma zona de quarentena que constitui um repositório de análise e processamento dos anexos infectados.

FUNÇÕES EXCLUSIVAS DO ANTIGEN DASYBARI PARA MICROSOFT EXCHANGE:

- Protecção total do sistema de armazenamento da Web do Exchange 5.5 e 2000, incluindo suporte para o Outlook Web Access.
- Tecnologias de múltiplos motores de análise para uma detecção exaustiva de vírus. Integra motores de análise de fornecedores líderes como a Norman Data Defense, Sophos, Computer Associates e Kaspersky Labs.
- Integra-se sem falhas com a API de Análise de Vírus do Microsoft Exchange 2000.
- Modos ESE e VS API seleccionáveis proporcionam aos administradores uma solução única de migração para o Microsoft Exchange2003, Exchange 2000 e 5.5.
- Proporciona protecção "prévia" através da análise de todas as mensagens de correio electrónico recebidas e enviadas no Internet Mail Connector (IMC) no Exchange 5.5 e no SMTP no Exchange 2000.
- Preparado para Empresas - consola do Antigen Central Manager, administração remota e actualizações automáticas dos motores de análise .
- Ideal para novos surtos de vírus antes de estarem prontos os ficheiros de definição.
- Elimina ficheiros, depura e/ou coloca em quarentena mensagens completas com base na correspondência do nome do ficheiro, tipos de ficheiro ou caracteres universais.
- Elimina e/ou coloca em quarentena mensagens completas com base no assunto, remetente ou nome de domínio.
- Os administradores podem definir três níveis de acesso: sem acesso, apenas leitura ou acesso completo.

Resumo das políticas de segurança implementadas

A actual plataforma de mail Exchange encontra-se configurada com o Anti Vírus Antigen, com o Anti Spam Exchange Intelligent Message Filter (IMF) e a lista de bloqueio de Spammers da Spamhaus.

Anti Vírus Antigen

Para um trabalho mais eficaz na detecção e remoção de Vírus, o Antigen utiliza os seguintes 5 file Scanners:

- CA Inoculatel T
- CA Vet
- Kaspersky
- Norman Data Defense
- Sophos Anti-Vírus

O Antigen também utiliza uma lista de detecção de Worms, a Sybari Worm List.

A actualização dos File Scanners e da Worm List é automática e está configurada para ocorrer 1 vez por dia entre as 00:00 e a 01:15. Quando estas são efectuadas, recebemos a actualização do dia anterior, que por sua vez, na sua grande maioria, detecta os vírus do dia anterior a esta.

Quando existem novos Vírus, com um grau de contaminação elevado, normalmente, os produtores de Anti Vírus apreçam-se a publicar novas actualizações, por vezes no próprio dia. Quando este tipo de situações ocorre, para além da actualização automática, são realizadas actualizações manuais.

Anti Spam – Lista da Spamhaus

A lista da Spamhaus, é uma lista que consulta várias listas de Spammers conhecidos.
Estas lista são constituídas por endereços identificados como fontes de SPAM e/ou situações irregulares de envio de mail como Open Relay.
Se um IP, que está referenciado nessas listas, tentar enviar mail através da nossa plataforma, o mesmo será recusado por este ter sido identificado como Spammer.

Anti Spam – IMF

O IMF é baseado na tecnologia Microsoft SmartScreen e inclui as seguintes caracteristicas:

- Heuristics-based analysis of messages determines whether they are legitimate or UCE.
- Server-side filtering with integrated Exchange Server administration.
- Support for per-message SCL allows thresholds to be set both at the server gateway running Intelligent Message Filter and at the user mailbox using Microsoft Outlook.

Esta ferramenta da Microsoft identifica e classifica as mensagens de Spam, que podem ser ignoradas, movidas para um directório ou directamente apagadas.

A classificação das mensagens é feita numa escala de 0 a 9 onde 9 quer dizer que tem 100% de certeza de que se trata de uma mensagem de Spam. Neste momento encontra-se configurado o nível 7 e todas as mensagens iguais ou superiores a esse nível são removidas da circulação dos nossos servidores de mail.

Essas mensagens são arquivadas e guardadas durante 7 dias, ao fim dos quais são apagadas.

A título de amostra, aqui ficam os números das mensagens de Spam identificadas e eliminadas automaticamente, pelos mecanismos acima referidos, durante o primeiro semestre de 2005:

- Janeiro 1.796.766
- Fevereiro 3.350.845
- Março 4.403.357
- Abril 6.009.609
- Maio 4.811.939
- Junho 5.184.078
- Julho 5.716.017

Apesar do gigantesco esforço que todos os ISPs do mundo fazem para combater esta praga de Vírus e Spam, é do conhecimento geral, que qualquer solução de Anti Vírus / Anti Spam não representa uma eficácia de 100% na detecção e eliminação do problema.

Encaramos com grande preocupação esta problemática e dada a complexidade do sistema, todas as reclamações e sugestões fornecidas pelos clientes são benéficas para a monitorização da eficácia dos nossos sistemas com vista ao seu melhoramento continuo.

Recomendamos vivamente a utilização adicional de sistemas de Anti Vírus / Anti Spam instalados nos computadores dos clientes, bem como, que estes sigam as politicas de segurança propostas pela Microsoft:
http://www.microsoft.com/portugal/seguranca

PAU - Politica Aceitável de Utilização

O provedor de serviços Internet (doravante ISP), alojamento de páginas web e outros serviços relacionados, oferece aos seus clientes os meios necessários para adquirirem e disseminarem informação pública, privada, comercial ou não comercial.

Sendo certo que, existem interesses divergentes relativamente a este assunto, o ISP reserva-se o direito de tomar determinadas acções preventivas ou correctivas.

Para tanto, e de forma a proteger todos estes interesses, foi criada a Política Aceitável de Utilização (doravante PAU), com o intuito de definir os direitos e deveres dos clientes que usam os nossos serviços.

Assim, o ISP reserva-se o direito de, sempre que exista violação das regras, infra referidas, remover os conteúdos ilegais, ou quaisquer outros que, da mesma forma, constituam uma violação da PAU ou que obstem ao normal funcionamento dos serviços prestados.

Pelo incumprimento de quaisquer dos direitos e deveres decorrentes da PAU incorre o cliente no pagamento de uma indemnização ao ISP, nos termos da Lei.

O ISP não poderá ser responsabilizada pelo incumprimento, por parte dos seus clientes, de quaisquer direitos ou deveres previstos na PAU.

A PAU tem carácter extra contratual e será revista periodicamente, pelo ISP, sem aviso prévio aos clientes.

Como anexo contratual, o cliente está implicitamente a aceitar a PAU, na versão original e consequentes versões que resultem da sua alteração.

Regras sobre Conteúdos

O ISP reserva-se o direito de remover quaisquer aplicações ou restringir a prestação dos Serviços quando tenha conhecimento da existência de actividades ilegais, desenvolvidas através desses meios, nomeadamente:

a) Violação de qualquer lei de qualquer jurisdição aplicável, incluindo leis sobre os conteúdos ou publicidade que podem ser difundidos na Internet, e ligadas a: álcool, concorrência, protecção de menores, substâncias ilícitas, exportação, armamento, importação, privacidade, títulos de crédito, telecomunicações e tabaco;
b) Prática de actos desonestos ou de qualquer forma injustos, incluindo a divulgação ou comunicação de informação difamatória, escandalosa, ameaçadora, injuriosa ou privada sem a permissão das pessoas afectadas, ou a divulgação de informação de tal forma que cause danos morais, quer devido à informação em si ou à frequência da sua divulgação;

c) Promoção, encorajamento ou defesa de violência contra qualquer estado, organização, grupo, indivíduo ou propriedade, ou divulgação de informação, formação ou apoio na concretização da referida violência;
d) Divulgação, envio ou recepção de informação que viole direitos de "copyright", patentes, "trademarks", marcas comerciais, segredos comerciais, acordos de licenciamento de software ou outros direitos de propriedade intelectual de terceiros;
e) Exposição pública do ISP ou do Grupo PT, das suas subsidiárias, dirigentes, empregados e/ou accionistas ao desprezo ou ridículo;
f) Programas, Scripts ou Aplicações que coloquem em causa o normal funcionamento dos serviços disponibilizados;
g) Participar ou permitir a realização de jogos de fortuna ou azar.

Regras sobre Segurança de Rede e Sistemas

1. Não é permitido ao utilizador a violação (ou tentativa de violação) de qualquer sistema de autenticação ou segurança que proteja contas de acesso, servidores, serviços ou redes. Nos casos de violação incluem-se, nomeadamente:

   a) Acesso não autorizados a dados alheios (quebra de privacidade);
   b) Pesquisa não autorizada de vulnerabilidades em servidores, serviços ou redes, nomeadamente detecção sistemática de resposta a serviços (Scan);
   c) Entrada ou tentativa de entrada em máquinas sem autorização expressa dos responsáveis (Break In);

2. Não é permitido ao utilizador interferir intencionalmente no bom funcionamento de utilizadores, servidores, serviços ou redes. Nestes casos incluem-se, nomeadamente:

   a) Acções de sobrecarga, combinadas ou não com exploração de vulnerabilidades de sistemas, que visem sabotar o funcionamento de serviços, (Denial of Service);
   b) Envio massivo de pacotes (Flooding);
   c) Quaisquer tipo de tentativas de entravar ou perturbar servidores, serviços ou redes;
   d) Instalação, Utilização e Disponibilização de PROXYS de uso da conectividade disponibilizada para outros fins que não os da utilização do serviço contratado;
   e) A manutenção de servidores OPEN RELAY;
   f) Introdução de vírus informáticos, "worms", código prejudicial e/ou "cavalos de Tróia";

3. Não é permitida a intercepção de dados em qualquer rede ou servidor sem autorização expressa dos legítimos proprietários.

4. Não é permitido falsificar (introduzir, modificar, suprimir ou apagar, no todo ou em parte) dados, após a sua produção, com intenção de iludir e induzir em erro os receptores desses dados. Nos casos de falsificação incluem-se, sem se limitarem a isso:

   a) Alteração de endereços IP (IP Spoofing);
   b) Alteração da identificação de mensagens de Correio Electrónico ou New.

Regras sobre Segurança de Serviços

Correio Electrónico

A utilização abusiva do correio electrónico pode causar transtornos e prejuízos aos restantes utilizadores da rede, quer directamente, quer indirectamente, ao pôr em causa o normal funcionamento dos sistemas de suporte ao serviço. Assim sendo, não é permitido:

a) O envio de mensagens de correio electrónico a quem tenha (expressamente) declarado não as desejar receber;
b) A difusão de uma mensagem ou de mensagens de teor igual ou idêntico para um número total de destinatários superior a 100, excepto em situações especiais devidamente reconhecidas como tal pelo ISP;
c) O envio de mensagens de dimensão superior a 20 MB, sem o acordo dos respectivos destinatários;
d) A utilização de outros servidores de correio electrónico que não os disponibilizados pela PT Prime para esse efeito, sem autorização (expressa) dos respectivos responsáveis;
e) A propagação de cartas em cadeia ou expedientes em pirâmide, quer o receptor aceite ou não o seu envio;
f) O cancelamento ou revogação de publicações ("postings") efectuados por outrem, com excepção dos cancelamentos ou revogações efectuados pelos moderadores de "newsgroups" ou "bulletin boards" quando no exercício das suas funções.

Propriedade dos endereços IP

O ISP mantém, controla e administra as gamas de endereços IP que lhe são atribuídos pelo RIPE, durante a vigência do período contratual., Assim, e com vista à correcta utilização dos Serviço, esta reserva-se o direito de alterar ou remover os referidos endereços IP, sempre que se verifique uma utilização incorrecta dos mesmos.